RECEIVED
CENTRAL FAX CENTER

SEP 3 0 2005

DILLON YUDELL LLP

ATTORNEYS AT LAW

USPTO FACSIMILE TRANSMITTAL SHEET

TO: Examiner Jung W. Kim	FROM: Andrew J. Dillon, Reg. No. 29,634
ORGANIZATION: US Patent and Trademark Office	DATE: September 30, 2005
ART UNIT: 2132 CONFIRMATION NO.:	TOTAL NO. OF PAGES INCLUDING COVER: 10
FAX NUMBER: 571-273-8300	APPLICATION SERIAL NO: 09/454,646
ENCLOSED: Appeal Brief	ATTORNEY DOCKET NO: RP9-98-055

☐ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

8911 N. CAPITAL OF TEXAS HWY., SUITE 2110, AUSTIN, TEXAS 78759
512.343.6116 (V) • 512.343.6446 (F) • DILLONYUDELL.COM

RECEIVED
CENTRAL FAX CENTER
SEP 3 0 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: **DAVID CARROLL CHALLENER**	§	Attorney Docket No. **RP9-98-055**
Serial No.: **09/454,646**	§	Examiner: **JUNG W. KIM**
Filed: **12/06/1999**	§	
For: **METHOD AND SYSTEM FOR IMPROVED COMPUTER SECURITY**	§	Art Unit: **2132**

APPEAL BRIEF

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Brief is submitted in support of the Appeal in the above-identified application:

Certificate of Transmission/Mailing

I hereby certify that this correspondence is being facsimile transmitted to the USPTO at 571-273-8300 or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on the date shown below.

Typed or Printed Name: Jane Graham *Date:* September 30, 2005 *Signature:* Jane Graham

RECEIVED
CENTRAL FAX CENTER

SEP 3 0 2005

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment, set forth at reel 010627, frame 0354.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-10 stand finally rejected as noted in the advisory action dated July 12, 2005. Claim 11 was previously canceled.

STATUS OF AMENDMENTS

No amendment to the claims has been submitted subsequent to the final rejection.

SUMMARY OF THE CLAIMED SUBJECT MATTER

The claims of the present application define a system and method for establishing a level of security in a personal computer, such as personal computer 10 depicted in Fig. 1 and described in the specification at Pages 11-12, Line 14 *et seq*. Personal computer 10 includes an operating system 22, as described at Page 13, Lines 4-7 and as illustrated in Fig. 2.

A variable security profile 70 is generated and stored by operating system 22 during Power On System Test (POST), when the computer system is turned on, as illustrated at block 50 in the flow chart of Fig. 3.

Security profile 70, as described in the specification at Page 14, Line 14 *et seq*., and as illustrated in Fig. 4 of the present application, includes a plurality of fields. Included within Security Profile 70 is tamper evident field 72 which is set if a physical security breach is detected. Field 74, as described at Page 16, Line 5 *et seq*., indicates the number of unsuccessful attempts at entering a user password which would be permitted before the system is shut down.

This field is described in the specification as being set by an operating system API "to take into account a greater security exposure during certain time periods, like late evening or on certain days, like week-ends." Security Profile 70 also includes a field 76 which specifies the security level of a user.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. The Examiner's rejection of Claims 1-9 under 35 U.S.C. §103(a) as being unpatentable over *Golding et al.*, United Stares Patent No. 5,265,163 in view of *Frisch*, Essential System Administration 2nd edition and the Examiner's rejection of Claim 10 under 35 U.S.C. §103(a) as unpatentable over *Golding et al*, in view *Frisch* and further in view of *Schmidt*, United States Patent Number 5,912,621, are to be reviewed on Appeal;

ARGUMENT

The Examiner has rejected Claims 1-9 under 35 U.S.C. §103(a) as being unpatentable over *Golding et al.*, United States Patent No. 5,265,163 in view of *Frisch*, Essential System Administration 2nd edition (hereinafter referred to as *Frisch*).

As noted above, Claims 1and 7, the independent claims in the present application, recite the provision of a variable security profile which is generated automatically when a personal computer system is turned on, wherein that variable security profile specifies "a variable number of unsuccessful power-on password attempts permitted based upon at least one other factor chosen from time of day and day of work; and, a security level authorization of the user." Thereafter, the user is allowed or denied use of the personal computer based upon compliance with that security profile. Thus, in accordance with the system and method claimed within the present application, a variable security profile is created which allows or denies a user access to the computer based upon two separate factors. The security level authorization of the user is one of those factors and, Applicant admits that allowing or denying access to a personal computer by a user based upon that user's security level authorization is well known in the art. However, the second factor specified within the claims of the present application is the setting forth of a variable number of unsuccessful power-on password attempts permitted based upon at least one other factor chosen from the time of day and the day of the week.

Golding et al. teach a computer system having a power-on password stored in non-volatile memory where an entry of the power-on password enables entry to the computer system. As admitted by the Examiner in Paragraph 7 of the Final Rejection dated April 29, 2005, "Golding does not teach a variable security profile wherein the variable security profile is automatically generated when the system is turned on, the variable security profile specifying: a variable number of unsuccessful power-on passwords permitted based upon at least one other factor chosen from time of day and day of week; and a security level of authorization of the user...." For this purpose the Examiner cites *Frisch* for its teaching of a security profile which locks an account after a specified number of consecutive invalid passwords are attempted. The Examiner believes it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the security profile taught by *Frisch* with the power-on password

check disclosed by *Golding et al.* Applicant also admits that specifying a variable number of permitted unsuccessful power-on password attempts prior to disabling the computer system is old and well known in this art.

However, Applicant respectfully urges the Board to consider that there is no suggestion within either *Golding et al.* or *Frisch* for varying the number of unsuccessful power-on password attempts permitted based upon a factor chosen from the time of day and the day of the week as expressly set forth in the present claims. To address this clear shortfall the Examiner notes that *Frisch* teaches that log in access may be restricted, based upon the time of day of the log in request. Citing *Frisch* at Pages 224-225, the Examiner notes that the system described therein teaches "limiting user access to certain days and/or times of day."

Applicant has urged the Examiner to consider that in such a situation *Frisch* may permit a user to continually generate unsuccessful power-on password attempts without incurring any action on the part of the system and, in response to that argument, the Examiner states a belief that by limiting user access to certain days and/or times of the day *Frisch* teaches that "the number of unsuccessful power-on password attempts permitted is zero, since the user is not allowed access; during non-restricted times, the number of unsuccessful power-on password attempts permitted by the user is zero or more, depending on the value specified by the C2 security-styled password restrictions." (See the continuation of Paragraph 11 of the Examiner's Advisory Action dated July 12, 2005.)

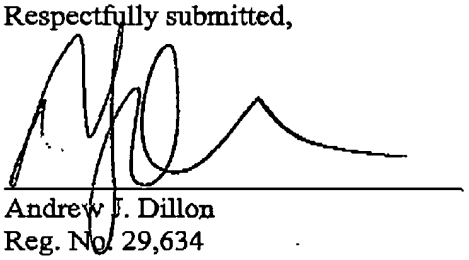
In that same paragraph, the Examiner has also noted that Applicant's assertion that an unlimited number of unsuccessful power-on attempts might be made during periods of time when the user is not allowed access to the computer and responded that "the disclosure of *Frisch* clearly discloses locking an account if the number of unsuccessful password attempts exceeds a number specified in the variable "MAXTRYS" and/or "u_maxtries", as described at Page 160 of *Frisch*.

Applicant respectfully urges that the Examiner cannot have this both ways. Either the number of unsuccessful power-on password attempts is specified within the profile of Frisch and that number of unsuccessful power-on password attempts will lock the system up during normal operating hours, or during periods of time when the user is not permitted to access the computer, or the user may be permitted an unlimited number of unsuccessful power-on password

attempts during those periods of time when access is not permitted. Nothing within *Frisch* shows or suggests in anyway changing the number of unsuccessful power-on password attempts from the specified number to zero during periods of time when the user is denied access to the computer. Indeed, it is the number successful power-on password attempts by the user which is limited to zero during periods of time when the user is denied access to the computer and Applicant urges the Board to reverse the Examiner's rejection of these claims based upon this faulty interpretation of the references by the Examiner.

The Examiner has cited *Schmidt* in combination with *Golding et al.* and *Frisch* against Claim 10 of the present application in that *Schmidt* teaches a computer system which is responsive to the removal of its physical case; however, Claim 10 depends, indirectly, from Claim 7 which, as noted above, recites expressly the variatión of the number of unsuccessful power-on password attempts which are permitted based upon: 1. the security level authorization of the user; and, 2. at least one factor chosen from time of day and day of week, as set forth expressly within Claim 7. Consequently, the Examiner's rejection of Claim 10 is not well founded and reversal of that rejection is respectfully requested.

Respectfully submitted,



Andrew J. Dillon
Reg. No. 29,634
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANT S

APPENDIX

1. A system for establishing a level of security in a personal computer having a memory and a stored operating system, the system comprising:

a variable security profile generated automatically when the system is turned on , said variable security profile specifying:

a variable number of unsuccessful power-on password attempts permitted based upon at least one other factor chosen from time of day and day of week; and,

a security level of authorization of the user; and

allowing or denying use of the personal computer to the user based on the security profile.

2. A system for providing security in a personal computer including the elements of claim 1 wherein the security profile includes a log of the access attempts for the personal computer and the results of each attempt.

3. A system of the type described in claim 2 wherein the variable security profile can be altered to a less secure state only by a system owner through the use of a password different than the password of the user.

4. A system of the type described in claim 3 for improving security of a personal computer wherein the variable security profile can be altered to a more secure state by a normal user.

5. A system for providing computer security including the elements set forth in claim 4 where the variable security profile includes a plurality of binary indicators have a more secure state and a less secure state, and a normal user of the computer system may change at least one of the binary indicators from a less secure state to a more secure state.

6. A system for providing computer security including the elements set forth in claim 5 wherein a user with a security password may change at least one of the binary indicators from a more secure state to a less secure state.

7. A method for providing improved security in a personal computer having an operating system and a security profile stored in memory, the steps of the method comprising:

automatically generating a variable security profile with indications of greater or lesser security when the personal computer is turned on, wherein the variable security profile specifies:

a variable number of unsuccessful power-on password attempts permitted based upon at least one other factor chosen from time of day and day of week; and,

a security level of authorization of the user;

storing the variable security profile in the personal computer;

using the variable security profile to determine what access, if any, a normal user will be permitted to have to the computer system; and

allowing the normal user to change the variable security profile from a level of lesser security to a level of greater security but denying the normal user permission to change the variable security profile from a level of greater security to a level of lesser security.

8. A method for providing security in a personal computer including the steps of claim 7 and further including the step of allowing a privileged user with a security password to change the variable security profile from a level of greater security to a level of lesser security.

9. A method of providing security in a personal computer including the steps of claim 8 and further including the steps of updating the variable security profile in response to a security risk.

10. A method of providing security in a personal computer including the steps of claim 9 and further including the step of responding to an attempt to open a cover of the personal computer and indicating the security risk associated with the attempt to open the cover in the variable security profile.

11. (canceled)

EVIDENCE APPENDIX

Other than the Office Action(s) and reply(ies) already of record, no additional evidence has been entered by Appellants or the Examiner in the above-identified application which is relevant to this appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings as described by 37 C.F.R. §41.37(c)(1)(x) known to Appellants, Appellants' legal representative, or assignee.